( Unclassified Paper )

NAVAL WAR COLLEGE
Newport, R.I.

# U.S. C$^4$I AND LOGISTICS VULNERABILITIES TO OFFENSIVE INFORMATION WARFARE

by

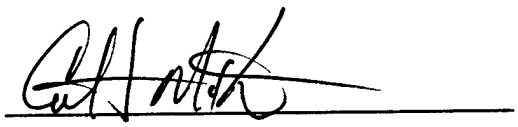
Colton McKethan

Lieutenant Colonel, United States Air Force

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.



Signature: 

13 June 1997

Paper directed by Captain George W. Jackson, USN
Chairman, Department of Joint Military Operations

**REPORT DOCUMENTATION PAGE**

| | |
|---|---|
| **1. Report Security Classification:** UNCLASSIFIED | |
| **2. Security Classification Authority:** N/A | |
| **3. Declassification/Downgrading Schedule:** N/A | |
| **4. Distribution/Availability of Report:** DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED. | |
| **5. Name of Performing Organization:** JOINT MILITARY OPERATIONS DEPARTMENT | |
| **6. Office Symbol:** 1C | **7. Address:** NAVAL WAR COLLEGE<br>686 CUSHING ROAD<br>NEWPORT, RI 02841-1207 |
| **8. Title** (Include Security Classification): U.S. $C^4I$ AND LOGISTICS VULNERABILITIES TO OFFENSIVE INFORMATION WARFARE (U) | |
| **9. Personal Author:** Lieutenant Colonel Colton McKethan, USAF | |
| **10. Type of Report:** FINAL | **11. Date of Report:** 13 June 1997 |
| **12. Page Count:** 30 | |
| **13. Supplementary Notation:** A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Joint Military Operations Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy. | |
| **14. Ten key words that relate to your paper:** Information Warfare; Command and Control Warfare; Computer Virus;Logistics; C4I; Vulnerabilities; Infowar; Intelligence; Revolution in Military Affairs; Technology. | |

**15. Abstract:** The information revolution fostered by the microchip has made it possible for military commanders to receive information in unequaled quantity and quality. U.S. commanders have a broad range of opportunities resulting from digitized technologies that enhance of military equipment performance and the application of force. These information advances represent force enablers providing synergistic advantage to operational command and control ($C^2$), intelligence, and logistic functions. However, there is a down side, in that the computers and microchips have vulnerabilities that must be addressed to retain operational force advantage.

Information warfare is central to the way the nation plans to fight in the future, and information systems now connect U.S. military forces on a worldwide basis. Despite the enhancements that connectivity brings, with integration of global communications, state and non-state actors are provided new ways to access and undermine the C2, intelligence, and logistics function via computer and communication networks. This new area of vulnerability extends from the strategic, through the operational, down the tactical levels of warfare. State and non-state actors have means of attacking core military centers of gravity and critical strengths without resorting to conventional attack or deception.

Today, joint commanders and civilian leaders must seriously consider the ramifications of unwanted intrusion into the national and defense information infrastructures. As U.S. forces become increasingly dependent on information to leverage battlespace awareness the need to protect information systems will increase. Backup capability must be designed into the information infrastructure to preclude erosion of force application capability.

| | | | |
|---|---|---|---|
| **16. Distribution / Availability of Abstract:** Unlimited | Unclassified<br>X | Same As Rpt | DTIC Users |
| **17. Abstract Security Classification:** UNCLASSIFIED | | | |
| **18. Name of Responsible Individual:** CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT | | | |
| **19. Telephone:** 841-6461 | | **20. Office Symbol:** C | |

Abstract of

U.S. $C^4I$ AND LOGISTICS VULNERABILITIES TO OFFENSIVE INFORMATION WARFARE

The information revolution fostered by the microchip has made it possible for military commanders to receive information in unequaled quantity and quality. U.S. commanders have a broad range of opportunities resulting from digitized technologies that enhance of military equipment performance and the application of force. These information advances represent force enablers providing synergistic advantage to operational command and control ($C^2$), intelligence, and logistic functions. However, there is a down side, in that the computers and microchips have vulnerabilities that must be addressed to retain operational force advantage.

Information warfare is central to the way the nation plans to fight in the future, and information systems now connect U.S. military forces on a worldwide basis. Despite the enhancements that connectivity brings, with integration of global communications, state and non-state actors are provided new ways to access and undermine the C2, intelligence, and logistics function via computer and communication networks. This new area of vulnerability extends from the strategic, through the operational, down the tactical levels of warfare. State and non-state actors have means of attacking core military centers of gravity and critical strengths without resorting to conventional attack or deception.

Today, joint commanders and civilian leaders must seriously consider the ramifications of unwanted intrusion into the national and defense information infrastructures. As U.S. forces become increasingly dependent on information to leverage battlespace awareness the need to protect information systems will increase. Backup capability must be designed into the information infrastructure to preclude erosion of force application capability.

# TABLE OF CONTENTS

# INTRODUCTION

***To win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill. Attack where he is unprepared; sally out when he does not expect you. Sun Tzu***

The information revolution brought about by the microchip has made it possible for military commanders to receive information in unprecedented quantity and quality. In the profession of arms, we base everything on information.[1] Warfare is about offense, defense, and exploitation of the enemy while managing one's own resources. Controlling, disseminating, denying, and even confusing information is essential to the conduct of military operations. U.S. military commanders have available a broad range of opportunities to conduct information warfare resulting from information technologies that enhance the performance of military equipment and the application of military force.[2] These information improvements represent force enablers providing synergistic advantage in the command and control, intelligence, and logistics functions.

The concept of information warfare is not new; military deception, psychological operations, and electronic warfare have been around for at least a half century. What is information warfare? Information warfare is any action to deny, exploit, corrupt, or destroy the enemy's information or information functions while protecting against exploitation of one's own military information functions.[3] Command and control warfare ($C^2W$), a subcomponent, applies key information warfare elements for military purposes.[4] The integration of computers and microchips, satellites, smart weapons, and artificial intelligence structures that make high-rate communications possible has transformed the way military commanders conduct operations and are central to the way the U.S. now conducts wars.

Today digital data energizes and enables the war making capabilities of the U.S. military forces; and at the heart of our command, control, communications, computers, and intelligence ($C^4I$) infrastructure and logistics system are the requirement for continuous flow of information. In the present high operational tempo (optempo) of warfare, the distribution process for information may be more critical for conducting synchronized joint military operations than at any time in the past. However, with a small investment of time, knowledge, and resources, either state or non-state actors may be able to effectively inhibit or counter our forces by employing offensive information warfare. [5]

Any adversary of the United States must probe for vulnerabilities in all areas including the information domain. Military campaigns against information dominant societies must incorporate measures designed to cripple the capacity of an information-based society from carrying out its information-dependent enterprises. [6] Critical information warfare vulnerabilities exist for the United States at all levels of war. The focus of this paper is on improved awareness of information warfare vulnerabilities at the operational level of war where campaigns and major operations are planned, conducted, and sustained to accomplish strategic objectives within a theater or area of operations. [7]

Here is the thesis: As the U.S. Armed Forces becomes more reliant on digitized data and electronic based digital data links in $C^4I$ and logistics, the operational military forces becomes more vulnerable to hostile intrusion that may damage, degrade, or destroy vital elements of the digitized data control system via offensive information warfare techniques. In this paper the U.S. military forces is the target of offensive information warfare.

## INFORMATION WARFARE IN MODERN COMBAT

***Probe him and learn where his strength is abundant and where deficient. I say victory can be created. For even if the enemy is numerous, I can prevent him from engaging. Sun Tzu***

In the United States, over 60 percent of the workforce is engaged in information-related management activities. No doubts exist that command and control warfare ($C^2W$) provides asymmetrical force enhancers that act as force multipliers on the modern battlefield. Today, military doctrine shaping the U.S. force structure and operation planning assumes information superiority especially at the operational level as stated in Joint Publication 1:

> The joint campaign should fully exploit the informational differential, that is, the superior access and ability to effectively use information on the strategic, operational, and tactical situation which advanced U.S. technologies provide our forces.[8]

In addition, Joint Vision 2010 provides a conceptual plan for leveraging technological opportunities to achieve new levels of effectiveness in joint warfighting that embodies the incorporation of improved $C^4I$ and goes on to develop four operational concepts: dominant maneuver, precision engagement, full dimensional protection, and focused logistics.[9]

However, state and non-state actors, hackers, U.S. radical militia and international terrorist groups, illegal drug organizations, organized crime and others aware of the advantages digital data brings can asymmetrically exploit the inherent weaknesses in our information dominant centers of gravity. Operational commanders must seek to protect critical nodes from offensive information warfare while exploiting the advantages that $C^2W$ operations bring. Offensive information warfare conducted by both state and non-state actors are designed to overcome existing operational and communications security protections. Today, most protections are dependent on individual personnel practices and installed firewalls to preclude unauthorized entry. However, it takes only one mistake to set off a

course of events that could undermine critical aspects of the U.S. $C^4I$ and logistics infrastructure that represent critical strengths, and in some cases military centers of gravity.

As U.S. forces become increasingly dependent on information to leverage battlespace awareness, command and control, and logistics support to operations through the Global Information Infrastructure (GII), the need to protect information systems will increase. Because information flow and knowledge are used to reduce the Clauswitzian "fog and friction" on the digitized battlefield, both become military critical factors. By attacking military informational centers of gravity at vulnerable points, state or non-state actors may be able to impede military actions at the operational level of war or even halt them. The far-ranging integration of the Global Information Infrastructure (GII) which shares information systems, creates vulnerabilities in the warfare system. The relationship between the civil/economic (national) and military information systems as depicted in Figure 1 below, highlights the extensive sharing between the two systems. Information infrastructure sharing, driven by reduced budgets, has led to unforeseen vulnerabilities and the potential for disruption of both the national and defense information systems.

Information based planning that assists the theater or joint force commander with knowing where to put forces and equipment, controlling their deployment and employment while protecting them is at the heart of GII. However, today at the operational level of warfare, the command and control, intelligence, and logistics functions have developed greater dependencies on computer and electronic transmission than at any time in the past.

## Global Information Systems and Relationships

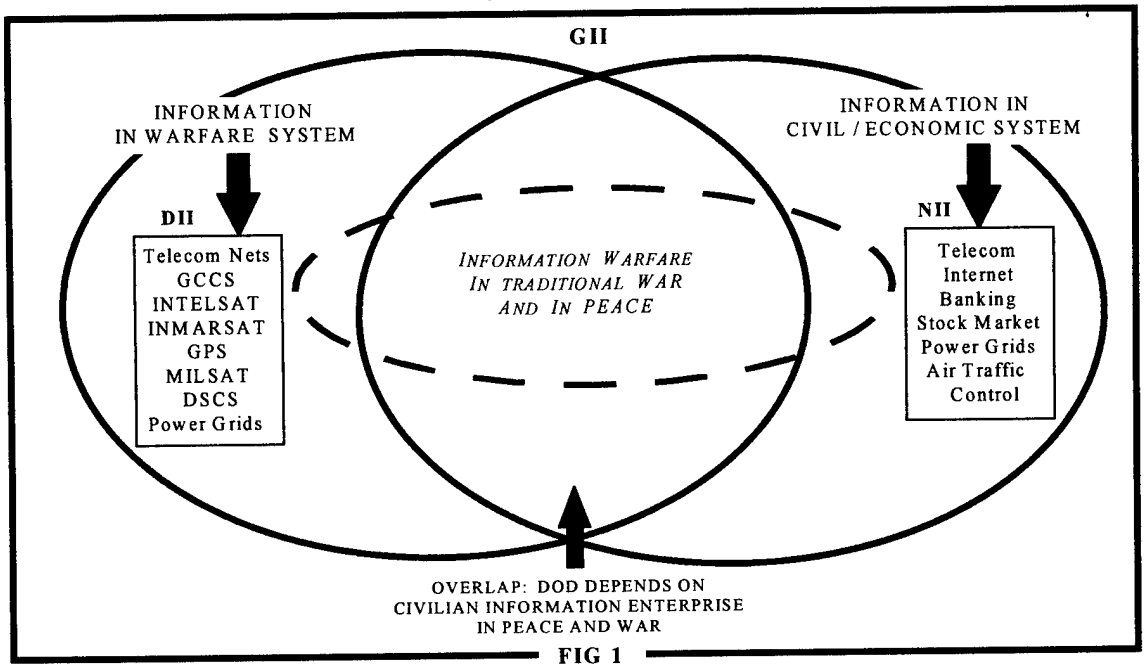



FIG 1

When directed against military operations in war, offensive information warfare undermines the ability to mass forces for maneuver, synchronization of force elements, provide security of operations, achieve battlespace awareness, and economically use force. One no longer need to attack the electrical power grid to degrade an operation. Simply by attacking the supporting communications and computer networks with offensive $C^2W$ the functions can be degraded or disrupted. If you have a vulnerability, your opponent will find it and exploit it.

## THE THREAT

***He who knows the art of the direct and the indirect approach will be victorious. Such is the art of maneuvering. Sun Tzu***

The modern military relies heavily on processing and transmission of vast amounts of information supporting operational missions. The greater the dependency of any nation on the integrity of its information infrastructure, the greater the risk of being paralyzed by attacks on the very things that helps provide its efficiencies. During May 1995, outgoing CIA Deputy

Director William Studeman stated that "massive networking makes the U.S. the world's most vulnerable target for information warfare." Studeman said, "our systems could be targeted by drug traffickers, organized crime, computer vandals, disgruntled employees, or paid professionals."[10] Attacks from a wide variety of sources appear to be growing, thereby confirming the offensive information warfare threat. Shown below in Figure 2,are a few of the growing number of incidents with the Defense Department often a major target.

## IW-Related Incidents

| | |
|---|---|
| • Hanover Hackers. | late 1980s |
| • Software time bombs in Public Network switches in Denver, Atlanta, and New Jersey. | mid - 1989 |
| • Dutch teenagers intrusion into Pentagon computers during the Gulf War. | Nov 1991 |
| • Rome Labs INTERNET intrusions. | Apr 1994 |
| • Organized crime attack on Citibank. | Aug 1994 |
| • INTERNET Liberation Front: 22-man group; 4 currently indicted. | Dec 1994 |
| • Numerous other hackers apprehended and awaiting prosecution (e.g. Mitnick, Poulsen). | Ongoing |
| • Sniffer programs found on all major INTERNET providers. | |
| • MCI Communications switch penetrations. | |
| • USAF Captain hacks into U.S. Atlantic Fleet ship computers as a test of system vulnerability. | Sep 1995 |
| • Los Alamos Computer break-in using unfixed UNIX sendmail | May 1996 |
| • Citibank seeks to prosecute $400,000 Russian hacker theft | Jun 1996 |

There Really Is A Smoking Gun

FIG 2

It would take only a handful of the "right" people, working with appropriate HUMINT to inflict enormous damage on our information based institutions. They could conduct their activities while working outside the United States, thousands of miles away, and leave no trace of the origin of the attack.

Offensive information warfare is attractive because it is cheap in relation to the cost of developing, maintaining, and using advanced military capabilities. Its cost little to create false

information, manipulate information, or launch malicious logic-based weapons against an information system connected to the globally shared telecommunications infrastructure. Personnel security practices often also invite attack. Many system managers may recall issuing directives that only authorized software may be loaded onto the organizations' computers, only to find later someone uploaded unauthorized software of unascertained origin. The preceding scenario represents one of many ways logic bombs, viruses, or hidden command code can gain acces and infect an otherwise secure system.

The danger posed by paid professionals taking advantage of security gaps in command, control, intelligence, and logistics computer systems, grows daily. In General Accounting Office (GAO) testimony to Congress, Jack Brock said, "Defense has already experienced what it estimates to be hundreds of thousands of computer attacks originating from network connections, some of which have caused considerable damage. Many of the so call hacker intrusions cost the Defense Department tens of millions of dollars, and pose a serious threat to U.S. national security."[11] Today, there are at least 25 countries with computer underground groups and these international hackers often are very sophisticated--sharing information and technologies for breaking into computers and computer controlled systems such as the internet.[12] Further, Defense officials and information security experts believe that over 120 foreign countries are developing information warfare techniques.[13] Figure 3 depicts the 1995 assessed capabilities of a few countries and their attributed information warfare capabilities. Figure 3 clearly demonstrates that where offensive information warfare capability is not resident in a given country, it is easily imported from

external sources. However, each nation listed in Figure 3 also has some inherent capability to conduct information warfare.

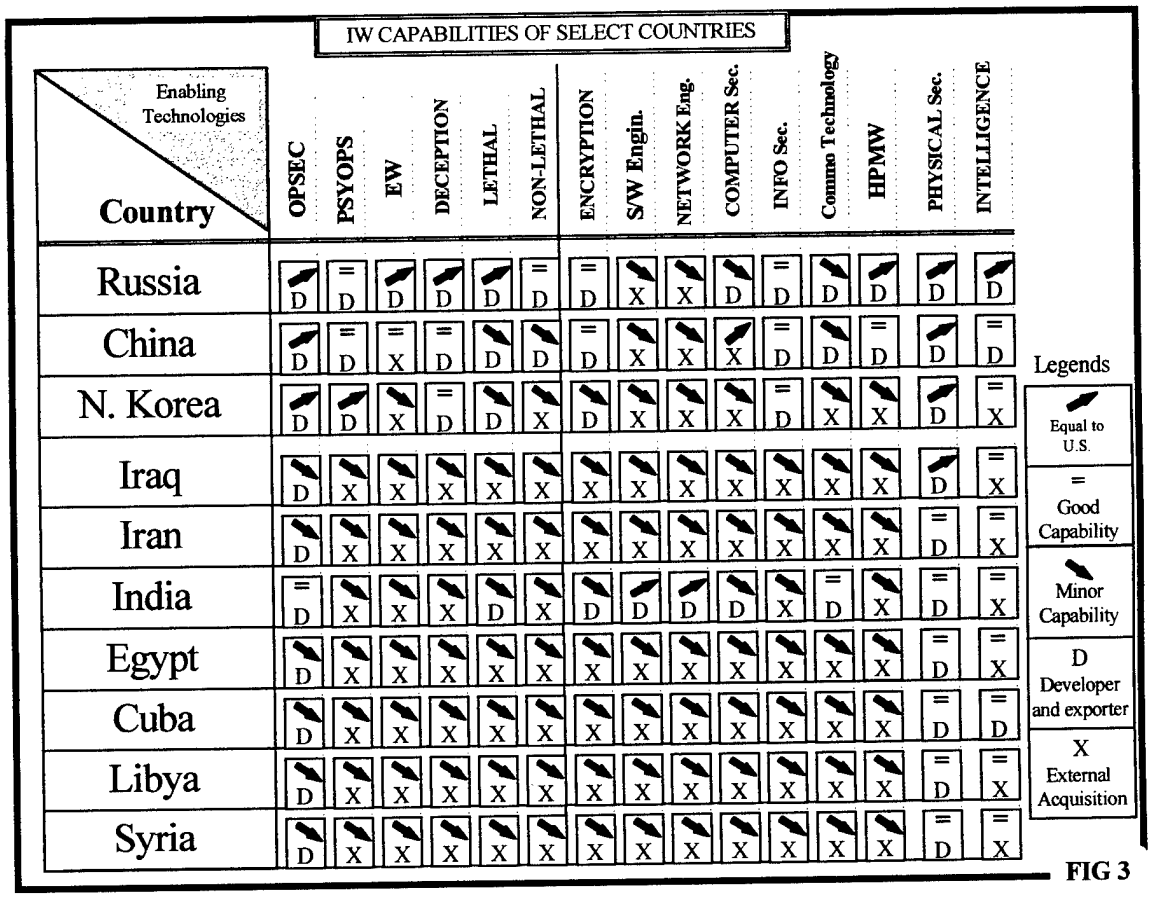


FIG 3

With the decline in the defense budget and the tremendous availability of dual use technologies in the commercial market, the DoD acquisition cycle has increasingly turned to commercial vendors to meet requirements for solid state microcircuitry. The dependence has led to greater vulnerabilities and further opens the door for the potential application of information warfare component chipping of solid state microcircuitry.

GAO reported to Congress the offensive information warfare danger to defense programs and military operations are worsening.

> Testifying in May 1996, GAO's Jack Brock said, "Air Force officials at Wright-Patterson Air Force Base reported that on average, they receive 3,000 to 4,000 attempts to access information each month from countries all around the world. Many attacks have been very serious. Hackers stole and destroyed sensitive data and software. They have installed 'backdoors' into computer systems which allow them to surreptitiously regain entry into sensitive Defense systems. They have 'crashed' entire systems and networks, denying computer service to authorized users and prevented Defense personnel from performing their duties." [14]

Computer attacks on the USAF Rome Laboratory demonstrate the potential of offensive information warfare.

> Rome Laboratory is the Air Force's premier command and control research facility. It works on very sensitive research projects such as artificial intelligence and radar guidance. Two computer hackers, one British and the other thought to be working for a foreign country used common hacker techniques, including loading "Trojan Horses" and "sniffer" programs to break into the lab's system. The hackers took control of the lab's network, and took all 33 subnets off-line for several days.
>
> During the attacks, the hackers stole sensitive air tasking order research data. Air tasking orders are the messages military commanders send during wartime to pilots; the orders provide information on battle tactics, such as where the enemy is located and what targets are to be attacked. The hackers also launched other attacks from the lab's computer systems, gaining access to systems at NASA's Goddard Space Flight Center, Wright-Patterson Air Force Base and Defense contractors around the country. No one knows what happened to the data stolen from Rome Laboratory. Rome lab's reported that if their air tasking order research project had been damaged beyond repair, it would have cost $4 million and 3 years to reconstruct it. [15]

In June 1996, the General Accounting Office(GAO) released a study highlighting the serious level of intrusions and the danger posed to the Defense Information Infrastructure that support the nations operational forces. GAO reported in its findings that the Defense Department is currently under information warfare attack and the attacks are proving destructive and costly. [16] Shown in Figure 4 is GAO's Information Warfare Assessment.

# IW Assessment - GAO Report

(Information Security: Computer Attacks at Department of Defense Pose Increasing Risks, 22 June 1996

Focus:

- Potential for further damage to DoD computer systems.
- Challenges DoD faces in securing sensitive information on its computer systems.

Findings:

- DoD relies on a complex information infrastructure to design weapons, identify and track enemy targets, pay soldiers, mobilize reservists, and manage supplies.
- Use of the INTERNET to enhance communications and information sharing has increased DoD exposure to attack.
- DoD information is unclassified, but it is sensitive, and should be protected.
- DISA estimates that DoD is attacked about 250,000 times per year, but only 1 in 500 attacks are detected and reported.
- Attackers have stolen, modified, and destroyed data and software, disabled protection systems, and shut down entire systems and networks.
- Security breaches cost DoD hundreds of millions of $$ annually, and pose a risk to national security, yet CERT teams are inadequately staffed, limiting response capability.
- Policy and training regarding computer security and network management are greatly outdated. There is no uniform policy for assessing risks, protecting systems, responding to incidents, or assessing damage.

**FIG 4**

Commanders must be aware that the fielded information dominant military equipment they depend on may not work when it is most needed. Consider the possibility of employing High Speed Anti-radiation Missiles (HARM) as part of a suppression of enemy air-defenses (SEAD) package and precision guided bombs to be used to destroy a key adversary's command and control (C2) node. Unknowingly, the microcircuits acquired in the defense acquisition cycle from a U.S. company were built by a foreign manufacturing subsidiary and chipped. As the air package goes into action against its target, radio frequency signals are emitted causing otherwise sound electronic circuits to disable firing or guidance components.

Think of the panic in the cockpits, the confusion of the targeteers, and the frustration of the air component or operational commander, as normally reliable systems do not work.

Commercial information products are extremely advanced and improving at an accelerated rate. As a result, use of commercial standards has proved more cost efficient than developing new MILSPEC electronic microprocessors and microchips. While military use of commercial equipment has its advantages, disadvantages are also apparent. The military drives neither the design nor the standards by which microchips are produced. Lack of military oversight makes it possible for introduction of logic bombs or chipping to occur during the production process. Flaws or hidden code can be introduced into an information based system by commission or omission. The effect of having certified weapons fail at the most inopportune time could put major military operations at risk of failure.

The Defense Science Board (DSB) reported that the vulnerability of the Department of Defense--and the nation--to offensive information warfare attack is largely a self-created problem. The DSB reported that:

> We have based critical functions on inadequately protected telecomputing services. We have created a target-rich environment and U.S. industry has sold globally much of the generic technology that can be used to strike these targets. Despite the risk, there still is inadequate understanding of the threat or the consequences of attacks on individual systems that have the potential to cascade throughout the larger enterprise. Further, the dependence of the Global Transportation Network (GTN) on unclassified data sources and the GTN interface to the Global Command and Control System (GCCS) leaves vulnerable vital components of the operational warfare complex to potential offensive information warfare. GCCS will continue to increase in importance, as it becomes the system of systems, through which CINCs, JTFs, and other commanders gain access to more and different information sources. Although GCCS has undergone selected security testing, much remains to be accomplished to reduce its vulnerabilities. The Global Combat Support System and a series of Advanced Concepts Technology Demonstrations currently shaping the future of $C^4I$ follows a remarkably similar process. Only those programs that can operate without

> connecting to the global network or those that can operate with an accepted level of risk in a networked information warfare environment should be built. Otherwise, we are paying for the means that an enemy can use to attack and defeat us. [17]

An effective operational C4 system is crucial to successful planning, preparing, conducting, and sustaining major operations or campaigns. Operations, logistics, and intelligence functions all depend on responsive C4 which requires a responsive C4 system. [18] The vulnerabilities of the U.S. command, control, communications, computers, and intelligence, surveillance, and reconnaissance ($C^4ISR$) system offers significant disadvantage for operational commanders and requires some detailed discussion.

## $C^4I$ SYSTEM VULNERABILITIES

***Thus what is of supreme importance in war is to attack the enemy's strategy. Sun Tzu***

In major operations or campaigns, when information of either strategic or of tactical importance is available to the commander, he can act decisively upon it. However, when information is not available, the commander can find himself unable to ascertain a true picture of the battlespace. Decisions made under stress are highly dependent upon the availability of information, validity, and timeliness; to achieve synergy the information must be integrated into force operations. The vulnerability of $C^4ISR$ to offensive information warfare stems from connectivity of computer based systems driven by interoperability requirements without fielded backup capability. The operational forces' commander, today, is dependent on a highly mobile system of forces capable of being moved from one theater of operations to another. By using enabling technologies such as distributed storage, responsive search mechanisms, and data interchanges the operational commander maximizes force employment potential.

The vulnerability of the $C^4ISR$ and logistic system stems from their supporting computer infrastructure. An adversary capable of disrupting the computer and communications networks is able to refuse key decisionmaking data from the operational commander. Without intelligence, the commander is blind--without logistics the commander cannot sustain himself. While information system advances allow the conduct of asymmetric warfare; if denied the advantages asymmetry brings, the commander must resort to conventional power. If command and control, intelligence, and logistics can be delinked from the supporting communications and computer infrastructure, then the commanders' operational responsiveness is inhibited. To visualize this idea, the supporting information system can be depicted as critical strengths surrounding the functional centers of gravity as shown in Figure 5 in a modified version of the Warden Five Rings Targeting Model.[19]

In military operation, the innermost three rings shown in Figure 5 are considered vital and usually well protected. Historically, $C^2$ has been attacked using direct force. Intelligence has been attacked by use of deception and secrecy, and logistics attacked through interdiction. Today with the use of computer viruses, worms, logic bombs, "Trojan Horses," or chipping techniques, state or non-state actors can affect the operational level commander's ability to control his forces without directly attacking $C^2$ and logistics nodes or engaging in operation deception. Offensive information warfare designed to degrade, disrupt, or destroy digital data or hardware is a likely candidate to augment and in some cases replace direct attack.

**Modified Warden Five Rings**
**Digital Data Information Warfare System**

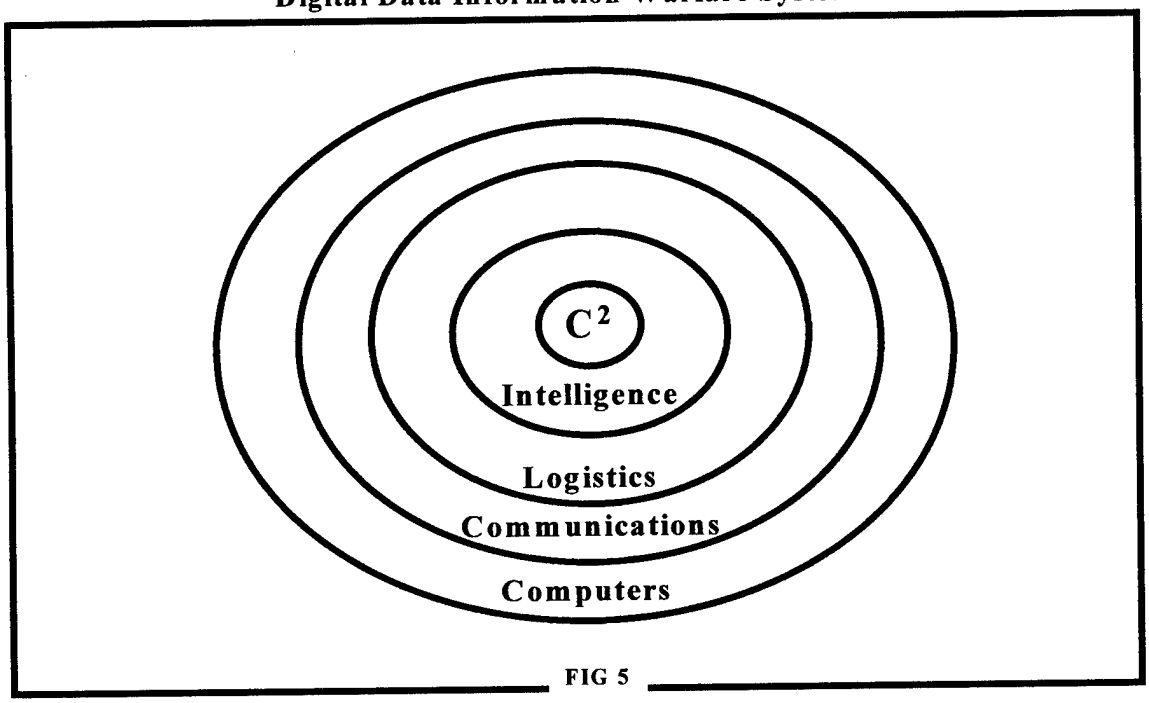



FIG 5

Acquiring intelligence information for use against the operational commanders is another way of getting inside his decision cycle. An example of the danger for operational forces, especially when working in security coalitions is demonstrated by a Reuters news story that reported that French military authorities suspect that unidentified hackers broke into their navy system in July 1995. Reportedly, the hackers tapped into data that provided details of the acoustic signatures of hundreds of French and allied ships. President Jacques Chirac ordered a major investigation. While American and British liaison officers, who provided information on their own vessels, were furious at the French suspected the Russians, some French officers suspect that the Americans were testing French security.[20] The GAO reported to Congress that intelligence gathering may be a prime function of many of today's hacker

attempts on military computer networks.[21] In contrast to the vulnerabilities of the $C^4I$ system, the logistics network faces even more serious problems.

## LOGISTICS SYSTEM VULNERABILITIES

Logistics are a critical element of combat power that assumes even greater importance at the operational level. Without adequate logistics, a major operation or campaign will sooner than later reach its culminating point, before assigned operational or strategic objectives are accomplished.[22] During OPERATION DESERT STORM nearly 25,000 shipping containers had to be opened merely to solve the mystery of what was inside. The Gulf War backlog resulted from non-automated receipt processing and lack of visibility.[23] To answer to this problem, Defense Logistics Agency and USTRANSCOM use an electronic Automated Manifest System that incorporates improved shipment planning and the ability to track and locate material in the logistics pipeline. Containers are coded with radio frequency tag information that can be read by laser bar code readers as any shipment moves via the International Transportation Information Tracking system (INTRANSIT). The INTRANSIT system culls tag information, stores, and updates data base to give complete visibility of cargo to the operational area commander.[24]

The threat to the logistics system today is more reality than security hype. Few are likely to forget the sensationalized news story which reported that according to Defense officials, a group of Dutch hackers offered to help Iraq during the Gulf War, by fouling up the Pentagon's logistics communications--25 percent of which were uncoded and sent on the Internet. Saddam refused the offer, thinking it to be a trick. The next time an offer is made--

rumor has it, Saddam is not likely to refuse.[25] The logistics process is virtually dependent on information as a force enabler. This dependence will continue to grow as "just in time" or focused logistics becomes reality. In addition, the push "to supply and sustain operational forces without prepositioning increases dependency on information asymmetrical advantages" without solving the underlying system vulnerabilities.[26]

The logistics system is tied together through interlinking digital data systems as shown in Figure 6 above, under centralized control of USTRANSCOM, a combatant commander.[27] Locating the USTRANSCOM master computer at Scott AFB, Illinois, roughly in the center

**MilAir and Sealift**
**Logistics Information Flow Structure**

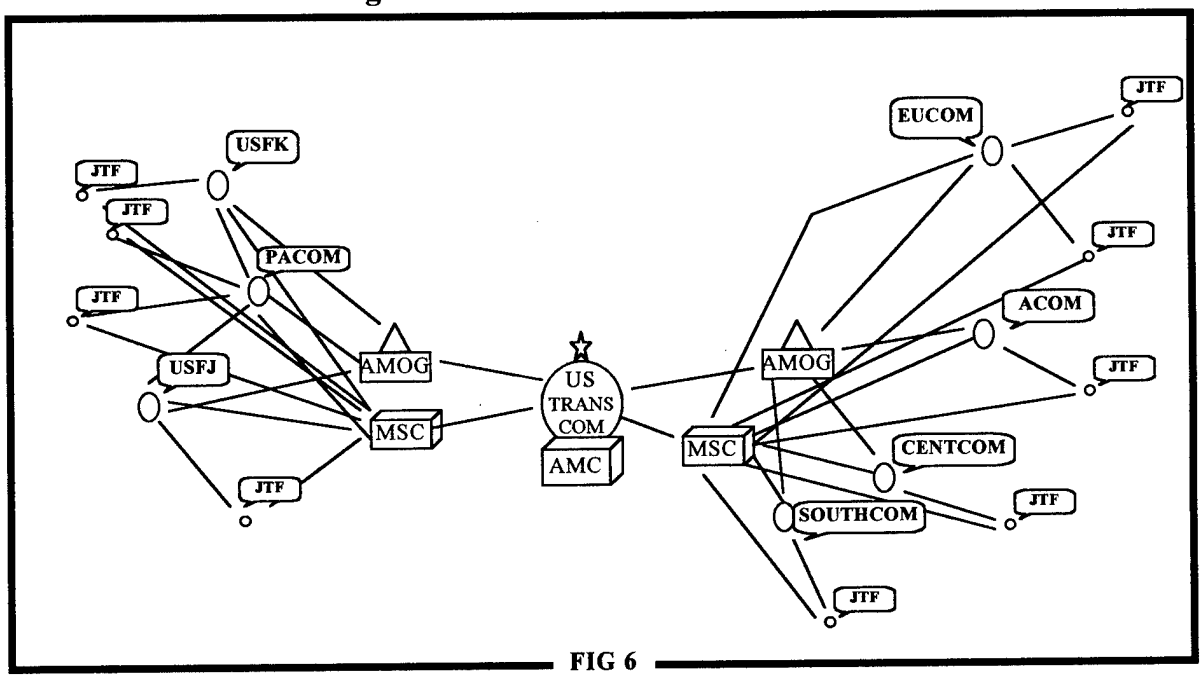



FIG 6

of continental United States, reduces an opponent's capability to directly attack the facility using conventional means. However, the control facility may be vulnerable to offensive

information warfare attack; either directed at the USTRANSCOM's Global Transportation Network (GTS), or the local commercial telephone exchange that serves as the backbone for the Command's communications connectivity. Few backups are in place or have been practiced for efficient use in the event telephone nets are unavailable.[28] Further, any node shown in Figure 6 or sealift vessel may be used as an entry point for offensive information warfare operations.

Redundancy in the switching networks reduces the current problem, but synchronized degradation against rerouting telecommunications net would force USTRANSCOM to seek alternative communications methods. Although alternate methods might sustain communications, they would place an onerous burden on operators working in unfamiliar and nonstandard communications flow and affect the logistic delivery and sustainment process.[29] Communications would not be halted, but transit processing would slow receipt of logistics on programmable schedules, affecting sequencing of operations and synchronization of forces. An offensive information warfare attack on the USTRANSCOM logistics tracking system could impede beans, bullets, and bombs from reaching sites where they are needed to bring them into operational play. Concurrently,should an attack be mounted upon the operational commanders $C^4I$, his ability to conduct warfare offensive operations is compromised.

The most vulnerable aspect of the operational level logistics network resides with the Military Sealift Command. The wide use of commercial shipping and harbor networks are extremely susceptible to intrusion and contamination. Cargo manifests are not handled via secure nets and are transmitted in the clear through the Stevedore Contract System at the dock.[30] With minor problems already existing in the shipping process, introduction of

computer viruses could serve to disrupt U.S. operational sealift. Other vulnerabilities exist using in the clear upload and download of data procedures from shipping company dock sites, as well as with the ship's computer. In the past, Military Sealift command used military installations to ship from; however, commercial ports throughout both coasts are widely used which undercuts the ability to thwart on-site intrusions.

To date, computer viruses, worms, Trojan Horses, logic bombs and chipping activities have not been detected in direct military attack against the U.S. logistics system. Rather, viruses are usually employed by mendacious users to attack digital data networks for personal gain, for the challenge, or for retribution from local or remote locations. Purposeful and or inadvertent contamination of computer disks, contaminated internet files, worms, planted chipping logic devices, and polymorphic and macro viruses are only a few ways that attack might be mounted against the logistics systems in its entirety or selectively.

## CONCLUSION

War is primarily concerned with two sets of activities--the delivery of energy and the communications of information. The energy dimension comes into play in warfare in its kinetic mode--largely as steel delivered at high velocity. The information dimension appears in numerous manifestations which usually fall into one of three categories--command and control, attacks on the opponent's information system, or leveraging of energy.[31]

According to Lt. Gen James Clapper, former head of Defense Intelligence Agency, as late as 1943 during World War II it took 9,000 2000-pound bombs dropped by 1,500 B-17 sorties to destroy a 60' by 100' target. By 1970, in Vietnam, it took 176 such bombs and 88

F-4 sorties to destroy the same target category. However, a mere 20 years later, in 1991 in DESERT STORM, it took only one or two laser-guided bombs in conjunction with a single F-117 sortie. The energy-information equation has been changed dramatically during the last three decades. The change is being driven by a single agent: solid state electronics.[32]

Digital data applications have become so critical to application of force at the operational level of war that if countermeasures are applied correctly the theater commander is robbed of the capability to effectively use his forces. By using offensive information warfare, adversaries can slow the theater commanders optempo as disrupted and viral infected computers and computer systems used to leverage information become useless. Further, degraded computer systems cause disruption to the theater commander's plan where considerable effort is made in positioning forces for precision engagement.

Should the commander lose trust in his information complex, planning efforts and strategies for force employment are also undermined. Most ominous is that degraded information systems disrupt the theater commander's ability to synchronize forces and leverage his information dependent systems as a force multiplier. Degraded and disrupted intelligence support systems adversely affect the commander's estimate of the battlespace by creating confusion and inaccuracy in the theater force commanders' assumptions. Ultimately, assumptions regarding the friendly and enemy situation, the direction and application of forces, and the projected outcome of military operations is shrouded in the fog of war and the commander can find himself unable to ascertain a true picture for decisionmaking.

The Defense Science Board, in its 1996 Information Warfare-Defense Report, assessed that the timing of an offensive information warfare attack is what may have strategic implications. In considering an attack on a port, the Board assessed:

> A power outage, communications failure, or road/rail disruption would be an inconvenience to citizens on an average day. However, these same incidents coordinated to occur at the peak of DESERT STORM deployments could easily have constituted a strategic threat which would have altered arrival of troops and equipment which played a critical part in the outcome of the war. Combine electric power grid attacks, attacks on harbor shipping systems with attacks on Pentagon computers, banking, and telephone switching systems, the result is a widespread loss of trust in the government's ability to respond to problems at home and abroad.[33]

There is no question that having information which allows you to operate faster or inside the decision cycle of an adversary is of inestimable value. However, keeping an adversary away from one's own information system vulnerabilities is as valuable, as having the ability to deny or delay an adversary's access to his own $C^4I$ or logistics systems. As the U.S. operational forces become more reliant on electronic information as a force multiplier, its $C^4I$ and logistics system become more vulnerable to hostile offensive information warfare attack.

Although there has been significant discussion of the merits of information warfare, much of it has been lost in debate on whether the United States Armed Forces is engaged in a Revolution in Military Affairs. Rather than bogging down in this often acrimonious discussion, a review of current capability and vulnerability is demanded. With the object of information warfare to control the capacity of an information based state to coordinate socially, economically, and militarily, offensive information warfare deserves careful study and countermeasure planning measures.

Recognition of the key areas of vulnerability and making them less vulnerable will require allocated resources and dedicated personnel to reduce vulnerability. Command, control, intelligence, and logistics functions remain vital in the conduct of operational level warfare; but, it is information driven asymmetries that yield the advantage for the U.S. military over potential adversaries. Failure to protect key centers of gravity and critical strengths may lead to early defeat of an otherwise superior armed force.

As the U.S. Armed Forces becomes more reliant on digitized data and electronic based digital data links in $C^4I$ and logistics, it becomes more vulnerable to hostile intrusion that may damage, degrade, or destroy vital elements of the digitized data control system through offensive counter information warfare techniques. Offensive information warfare is a relatively cheap way for either state or non-state actors to attack the United States and disrupt the very core of its strengths.

## Notes

1. Department of the Air Force, Information Warfare, Headquarters U.S. Air Force/ XOXD, Pentagon (Washington, DC: 1996), p. 1.

2. Ibid, p 1.

2. Ibid, p.5.

4. Office of Chairman, Joint Chiefs of Staff, Doctrine for Joint Operations, Joint Publication 3-0 (Washington DC: 1 February 1995) p. GL-5.

5. Telephone conversation with Dr. Fred Giessler, National Defense University School of Information Warfare, Washington, DC, 28 March 1997.

6. Defense Science Board, Report of the Defense Science Board Task Force on Information Warfare - Defense (IW - D) (U), Office of the Under Secretary of Defense for Acquisition & Technology, (Washington, DC: November 1996), p. 2-1.

7. Joint Publication 3-0, pp. GL-10/11.

8. Defense Science Board, Report on IW-D, p. 2-1

9. Ibid, p. 2-1.

10. Daniel Brandt, "Infowar and Disinformation: From the Pentagon to the Net," Namebase Newsline, No. 11, October-December 1995 <http://www.berkeleynetcentral.com /DrPseudocryptonym/infowar.html>, (9 May 1997), p. 2.

11. Jack L. Brock, Jr., "Testimony," Permanent Subcommittee on Investigations, Committee on Governmental Affairs, U.S. Senate, INFORMATION SECURITY: Computer Attacks at Department of Defense Pose Increasing Risks, Hearings (Washington DC: Federal Document Clearing House, INC: 22 May 1996), p. 3.

12. Office of the Under Secretary of Defense, 1994 DSB Summer Study on Information architecture for the Battlefield--Final Report (U), Report to the Secretary of Defense, (Washington, DC: October 1994), p. B-5.

13. Brock, p. 6.

14. Ibid, p. 4.

15. Ibid, pp. 4, 5, and, 6.

16. Defense Science Board, Report on IW-D, p. A-6.

17. Ibid, p. 2-2.

18. Milan Vego, Operational Functions, Joint Military Operations Department, Naval War College: (Newport RI: August 1996), p. 12.

19. Note: Colonel (Ret) John Warden, III, Former Commandant of the USAF Air Command and Staff College developed a concept model of five concentric and interwoven rings for targeting a nations key centers of gravity in warfare.

20. Brandt, p. 3.

21. Brock, p. 6.

22. Vego, p. 29.

23. Department of Defense, Defense Logistics Agency: Keeping Our Forces Ready for War & Peace, Defense 97 Issue 1, Alexandria, VA, p. 21.

24. Ibid, p. 23.

25. John J. Fialka, "Pentagon Studies Art of Information Warfare to Reduce its Systems Vulnerability to Hackers," Wall Street Journal, 3 July 1995, p. A12.

26. General John M. Shalikashvili, "Chairman of Joint Chiefs of Staff Lecture, U.S. Naval War College, Newport, RI: 29 April 1997.

27. Interview of Lt Colonel Olen Scott Key, Naval War College, Newport, RI, 10 March 1997 and Lt Colonel Mark Johnston, USTRANSCOM, Scott AFB, IL, 9 May 1997.

28. Telephone conversation with Lt Commander John M. Jorgensen, USN, USTRANSCOM, Scott AFB, IL, 12 May 97.

29. Ibid

30. Telephone conversation with Doug Loyd, Commander, USN, Naval War College, Newport, RI, 3 May 97.

31. Abe Singer and Scott Rowell, "Information Warfare: An Old Operational Concept With New Implications." Strategic Forum, National Defense University Institute for National Strategic Studies, Number 99, December 1996, p. 2.

32. Ibid

33. Defense Science Board, Report on IW-D, p. A-12.

## Bibliography


Brandt, Daniel. "Infowar and Disinformation: From the Pentagon to the Net." Namebase Newsline. No. 11, October-December 1995. <http://www.berkeleynetcentral.com /DrPseudocryptonym/infowar.html>. (9 May 1997).

Defense Information Systems Agency, Joint Interoperability and Engineering Organization, and Center for Information Systems Security. Planning Considerations for Defensive Information Warfare - Information Assurance, Task Order 90-SAIC-019, Contract No. DCA 100-90-C-0058, Washington, DC: 1993.

Defense Science Board. Report of the Defense Science Board Task Force on Information Warfare - Defense (IW - D) (U). Office of the Under Secretary of Defense for Acquisition & Technology. Washington, DC: 1996.

Elam, Donald Emmett. Attacking the Infrastructure: Exploring Potential Uses of Offensive Information Warfare. Unpublished Research Paper, Naval Postgraduate School Monterey, California: 1996.

Fialka, John J. "Pentagon Studies Art of Information Warfare to Reduce its Systems Vulnerability to Hackers." Wall Street Journal, 3 July 1995, p. A12.

Interview of Lt Colonel Olen Scott Key, Naval War College, Newport, RI, 10 March 1997

Jorgensen, John M., Lt Commander, USN and Steve Hofmann, Lt Colonel, USAF. "Events Logbook: A Groupware Solution for Command and Control." U.S. Transportation Command. Scott AFB, Illinois: 1997.

Office of the Chairman, Joint Chiefs of Staff. Joint Pub3.0, Doctrine for Joint Operations. Washington, DC: 1995.

Office of the Under Secretary of Defense. 1994 DSB Summer Study on Information Architecture for the Battlefield--Final Report (U), Report to the Secretary of Defense. Washington, DC: 1994.

Rowell, Michael O., Major, USMC. "Animal Crackers: Weaknesses in our C4I Strengths." Unpublished Research Paper, U.S. Naval War College, Newport, RI: 1995.

Shalikashvili , John M., General., "Chairman of Joint Chiefs of Staff." Lecture. U.S. Naval War College, Newport, RI: 29 April 1997.

Singer, Abe and Scott Rowell. "Information Warfare: An Old Operational Concept With New Implications." Strategic Forum, National Defense University Institute for National Strategic Studies, Number 99. Washington, DC: December 1996.

Sun Tzu. The Art of War, trans. by Samuel B. Griffith. New York: Oxford University Press, 1963.

Szafranski, Richard, Colonel, USAF. "An Information Warfare SIIOP." 14 September 1996. <http://www.infowar. com.mil_c4i/szfran.html-ssi> Air War College, Maxwell AFB, Alabama. (9 May 1997).

Telephone conversation with Dr. Fred Giessler, National Defense University School of Information Warfare, Washington, DC. 28 March 1997.

Telephone conversation with Commander Doug Loyd, USN, Naval War College, Newport, RI. 3 May 97.

Telephone conversation with Lt Colonel Mark Johnston, USTRANSCOM, Scott AFB, IL. 9 May 1997.

Telephone conversation with Lt Commander John M. Jorgensen, USN, USTRANSCOM, Scott AFB, IL. 12 May 97.

U.S. Congress. Senate. Permanent Subcommittee on Investigations, Committee on Governmental Affairs. INFORMATION SECURITY: Computer Attacks at Department of Defense Pose Increasing Risks. Hearings. Washington DC: Federal Document Clearing House, INC: 1996.

U.S. Department of Defense. "Defense Logistics Agency: Keeping Our Forces Ready for War & Peace." Defense 97, Issue 1. Alexandria, VA: 1997.

U.S. Department of the Air Force. Information Warfare. Washington, DC: 1996.

Vego, Milan N. Operational Functions, JMO Department. Newport, RI: Naval War College, 1996.

Warden, John, III, "Employing Air Power in the Twenty-first Century," The Future of Air Power in the Aftermath of the Gulf War, Air University Press, 1992.

# APPENDIX A

## Definition of Terms

**Bit Flipping** - The use of microwave beams as a method to attack computers so that they generate random errors.

**Chipping** - The act of inserting hidden code onto a clean and otherwise operable microchip that is designed to respond to a trigger mechanism.

**Computer Virus** - Malicious computer code that attaches itself to system or application program blocks of code in order to propagate. Viruses have four characteristic components:

- *Self reproducing* and capable of moving from one part of the host computer system to another. Unlike worms, viruses must be downloaded and physically inserted into a new host computer or electronically transmitted to another host for infection transmission.
- *Capable of self replication* regardless of whether replication is required to fulfill its mission.
- *Mission integral* must perform a function unexpected and often undesired by the systems owner.
- *Trigger* mechanism may or may not be present.

**Flying Dutchman** - A type of Trojan Horse that erases all traces of itself after performing its mission and frustrate subsequent investigations.

**Information Warfare** - Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems, and computer-based networks. [CJCSI 3210.01, 1996]

- *Command and Control Warfare* a sub-component of Information Warfare does not f ully overlap the IW domain. JCS MOP 30 defines five pillars that comprise $C^2W$: Electronic Warfare, Deception, Security, PSYOPS, and Physical Destruction. Its objective is to decapitate the enemy's command structure from its forces.

**Hacker** - Individual who conducts unauthorized entry into a computer system or network.

**JAVA** - An object oriented, platform-independent programming language, often used to create small cross-program executable software applications called applets that are downloaded from remote sites and that execute automatically.

**Logic Bomb** - Malicious computer code that may or may not be a virus whose mission component is triggered by a true/false condition which destroys a computer's programs and data. A type of Trojan Horse that does not propagate.

**Malicious Computer Code** - Computer code deliberately placed on a computer system without permission of the owner.

**Polymorphic Virus** - Computer viruses that is designed to avoid signature-based detection scanning by not leaving any predictable sequence of instructions that a virus scanner can optimize as a detection algorithm.

**Sniffer** - A sniffer sits on a host network and collects passwords and other similarly revealing information.

**Time Bomb** - A coded subset of a logic bomb which usually uses either date and/or time as its trigger mechanism.

**Trojan Horse** - Hidden malicious computer code that is located within a block of code in any application program or system program that is unknown to the owner and designed to perform an act unexpected by the owner.

**Trap Door** - Hidden computer code designed to allow circumvention to system security measures. May be a legitimate programmed code designed to allow a developer to bypass lengthy log-on routines or to access source computer codes directly. If known by unauthorized persons, these codes may offer a significant source for a security breech.

**Worm** - Malicious computer code that operate independently of system computer programs and may or may not have a mission component or trigger mechanism. Similar to a computer virus, it can replicate itself and can mail replicas of itself outside the host system.